The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
10/07/2020

SUBJECT:
Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary code execution. Google Chrome is a web browser used to access the Internet. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Google Chrome versions prior to 86.0.4240.75

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary code execution. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Details of the vulnerabilities are as follows:

- A use-after-free vulnerability. Specifically, this issue exists in the 'payments' component. (CVE-2020-15967)

- A use-after-free vulnerability. Specifically, this issue exists in the 'Blink' component. (CVE-2020-15968)
- A use-after-free vulnerability. Specifically, this issue exists in the 'WebRTC' component. (CVE-2020-15969)
- A use-after-free vulnerability. Specifically, this issue exists in the 'NFC' component. (CVE-2020-15970)
- A use-after-free vulnerability. Specifically, this issue exists in the 'printing' component. (CVE-2020-15971)
- A use-after-free vulnerability. Specifically, this issue exists in the 'audio' component. (CVE-2020-15972)
- A use-after-free vulnerability. Specifically, this issue exists in the 'autofill' component. (CVE-2020-15990)
- A use-after-free vulnerability. Specifically, this issue exists in the 'password manager' component. (CVE-2020-15991)
- A security-bypass vulnerability that occurs due to insufficient policy enforcement. Specifically, this issue exists in the 'extensions'. (CVE-2020-15973)
- An integer-overflow vulnerability. Specifically, this issue exists in the 'Blink' component. (CVE-2020-15974)
- An integer-overflow vulnerability. Specifically, this issue exists in the 'SwiftShader' component. (CVE-2020-15975)
- A use-after-free vulnerability. Specifically, this issue exists in the 'WebXR' component. (CVE-2020-15976)
- A security vulnerability. Specifically, this issue occurs due to certain inappropriate implementation in networking. (CVE-2020-6557)
- A security vulnerability because it fails to properly validate data. Specifically, this issue exists in the 'dialogs' component. (CVE-2020-15977)
- A security vulnerability because it fails to properly validate data. Specifically, this issue exists in the 'navigation' component. (CVE-2020-15978)
- A security vulnerability. Specifically, this issue occurs due to certain inappropriate implementation in the 'V8' component. (CVE-2020-15979)
- A security-bypass vulnerability that occurs due to insufficient policy enforcement. Specifically, this issue exists in the 'Intents' component. (CVE-2020-15980)
- A security vulnerability that occurs due to an out-of-bounds read error. Specifically, this issue exists in the 'audio' component. (CVE-2020-15981)
- An information-disclosure vulnerability that occurs due to a side-channel information-leakage condition. Specifically, this issue exists in the 'cache' component. (CVE-2020-15982)
- A security vulnerability because it fails to properly validate data. Specifically, this issue exists in the 'webUI' component. (CVE-2020-15983)
- A security-bypass vulnerability that occurs due to insufficient policy enforcement. Specifically, this issue exists in the 'Omnibox' component. (CVE-2020-15984)
- A security vulnerability. Specifically, this issue occurs due to certain inappropriate implementation in the 'Blink' component. (CVE-2020-15985)
- An integer-overflow vulnerability. Specifically, this issue exists in the 'media' component. (CVE-2020-15986)
- A use-after-free vulnerability. Specifically, this issue exists in the 'WebRTC' component. (CVE-2020-15987)
- A security-bypass vulnerability that occurs due to insufficient policy enforcement. Specifically, this issue exists in the 'networking' component. (CVE-2020-15992)

- A security-bypass vulnerability that occurs due to insufficient policy enforcement. Specifically, this issue exists in the 'downloads' component. (CVE-2020-15988)
- An unspecified security vulnerability that exists in the 'PDFium' component. (CVE-2020-15989)

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:
The following actions should be taken:
- Apply the stable channel update provided by Google to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Google:
https://chromereleases.googleblog.com/2020/10/stable-channel-update-for-desktop.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15967
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15968
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15969
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15970
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15971
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15972
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15990
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15991
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15973
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15974
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15975
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15976
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6557
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15977
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15978
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15979
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15980
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15981
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15982
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15983
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15984

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15985
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15986
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15987
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15992
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15988
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15989